In the claims:

1. (previously presented) A method of securing packet data transferred between a group of stations over on a backbone, the backbone comprising an ingress point and egress point, the method comprising the steps of:

receiving, at the ingress point of the backbone, group security association data associated with the group of stations;

receiving a packet at the ingress point of the backbone, a packet including a group identifier corresponding to the group of stations and a destination address for the packet;

transforming, at the ingress point of the backbone, the packet according to the group security association associated with the group identifier, wherein the ingress point is a provider edge device; and

forwarding the transformed packet over the backbone using the group identifier as a backbone address.

2. (previously presented) The method according to claim 1, wherein the step of transforming includes the step of retaining fields of the packet needed to transfer the packet to the destination address over the backbone.

3. (cancelled)

4. (cancelled)

5. (cancelled)

6. (previously presented) A method of securing packet data transferred between a group of stations of a private network on a backbone, the backbone comprising an ingress and egress, the method comprising the step of:

receiving, at the egress point of the backbone, group security association data for the group of stations, wherein the egress point is a provider edge device;

receiving a packet at the egress of the backbone, the packet including an identifier of the group of stations and a destination for the packet;

. restoring the packet responsive to the group security association data associated with the identifier of the group of stations; and

forwarding the packet to the destination.

7. (cancelled)

8. (cancelled)

9. (cancelled)

10. (previously presented) A network architecture for providing secure communication between at least two members of a private network over a communication link, the network architecture comprising:

a first station;

an ingress point to the communication link wherein the communication link comprises a plurality of provider devices, and wherein the ingress point is one of the plurality of provider devices;

an egress point from the communication link;

a second station, coupled to the egress point;

a group security association, corresponding to a group of stations in a private network, both the first station and the second station being members of the group and wherein a group identifier is associated with the group;

means for securing data transferred between members of the group from the ingress point and the egress point in the network using the group security association by transforming the data at the ingress point using a group security association associated with the group identifier;

means for forwarding the communication between members of the group over the network using a group address associated with the group, the group address including the group identifier and a group destination address.

11. (cancelled)

12. (original) The network architecture of claim 10, wherein the communication link comprises a plurality of provider devices, and wherein the egress point is one of the plurality of provider devices.

13. (original) The network architecture of claim 10, wherein the group comprises at least three stations.

14. (cancelled)

15. (cancelled)

16. (original) The network architecture according to claim 10 wherein the means for securing data includes transform logic for encrypting only a portion of data transferred between the ingress point and egress point of the communication link.